How Does Flock Work?

October 20th, 2025, by Brendan Trachsel

Outline

- What are ALPRs?
- Flock & the 4th Amendment
  - How Flock tracks you
  - The vehicle-to-person pipeline
  - What courts are saying
- What happens to your data once it’s entered into Flock’s Database
  - A look into Flock’s patent
  - Who owns the data?
  - Abuse & failure
- How your data is shared with outside agencies
  - Risk of federal access
- What can you do now?

What are ALPRs?

(Automated License Plate Readers)

Comparing Traditional LPRs and ALPRs

“Traditional” LPRs

- Scan the license plates of every car that passes them
- Checks plate scans against hotlists
  - Warrants, stolen vehicles, amber alerts, etc.
- Alerts agencies of any “hits”
- Scans that are not hits are deleted

ALPRs, like Flock

- Scan the license plates of every car that passes them
- Checks plate scans against hotlists
  - Warrants, stolen vehicles, amber alerts, etc.
- Alerts agencies of any “hits”
- **All scans are kept for at least 30 days**
  - **Also used to train their AI model**
- **Flock’s AI system categorizes all data**
  - **“Vehicle Fingerprint”**
- **All information is available & searchable via Flock’s AI-powered database**
- **Available to outside agencies**

Flock & the 4th Amendment

The 4th Amendment

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

- Government wants to search? They need a Warrant.
    - With exceptions: plain view, consent, exigent circumstances, third-party doctrine, etc.

Undeniable: Flock Tracks You

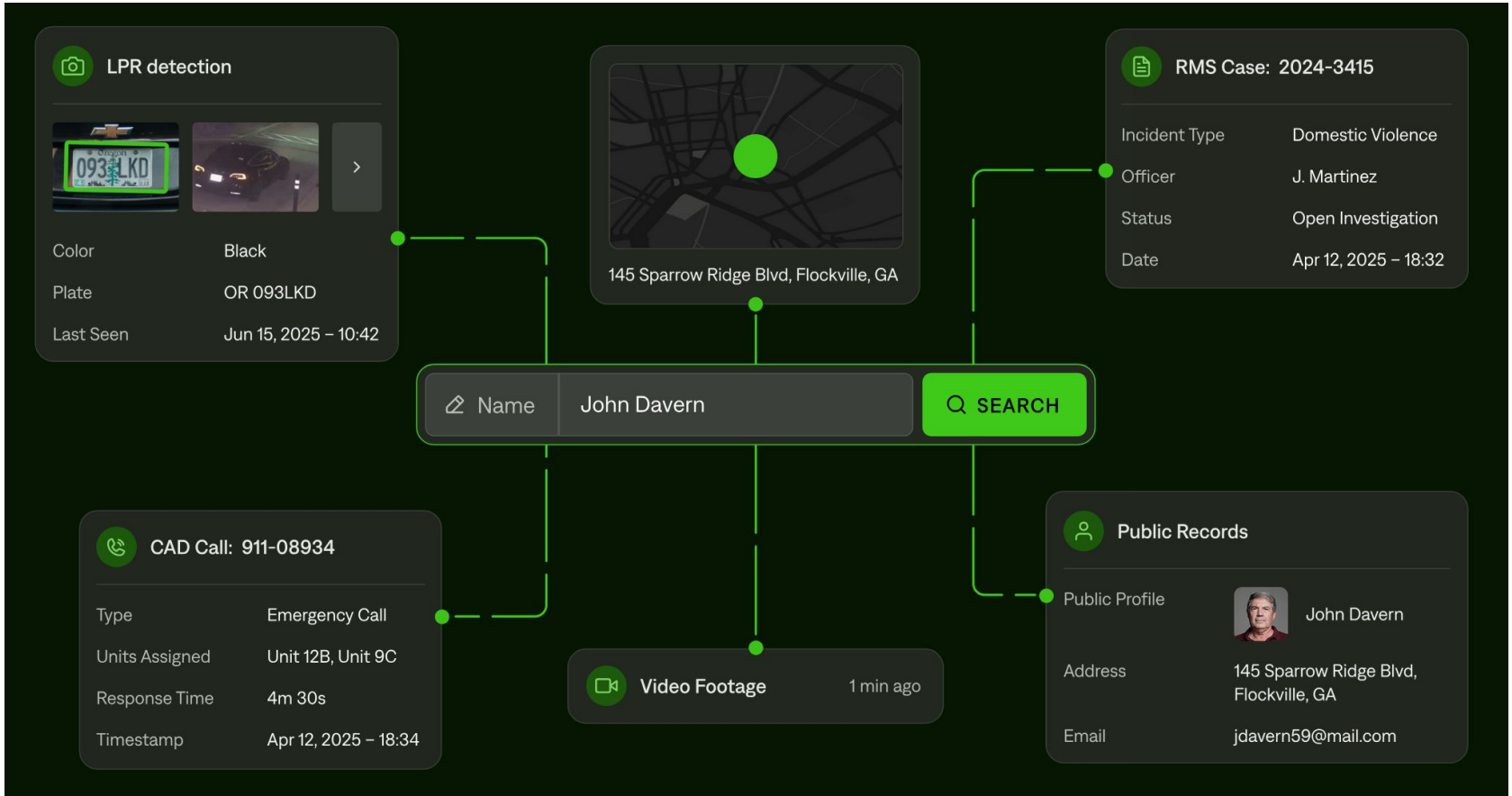
Flock & Flagstaff PD state that ALPRs are not tracking technology, rather that they only take single point-in-time photos from fixed locations.

- Daisy-chaining multiple cameras at every major intersection that feed into one database is merely tracking through a checkpoint-based system
  - This is supported by Flock's own patent on their technology
  - They also record video now!
- This means that even if you're not doing anything wrong, your movements are still being tracked and stored, often for long periods of time.

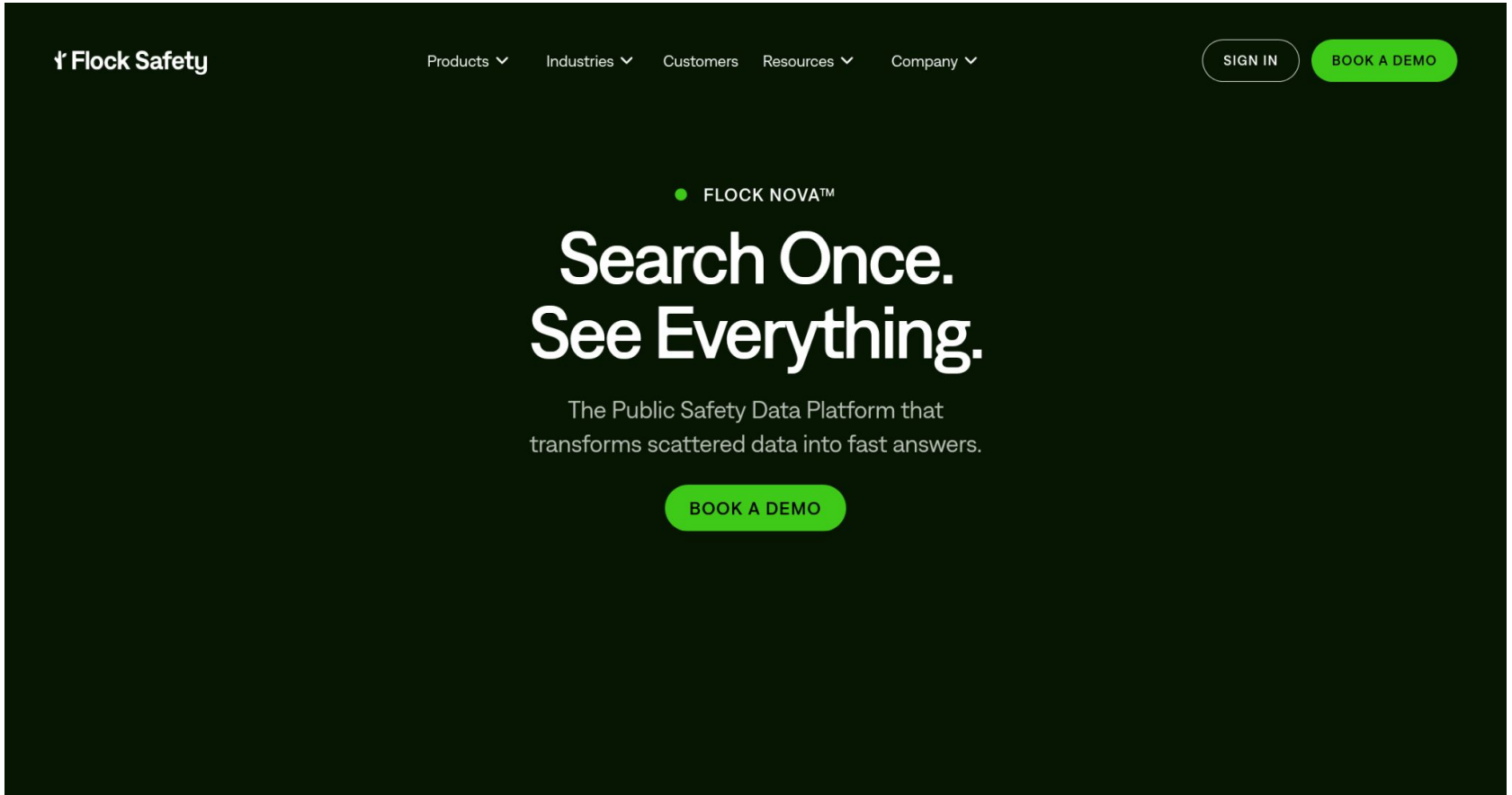
Not Just Your Car: The Vehicle-to-Person Pipeline

Flock Nova, their nationwide person lookup tool, collects data through public records, private data brokers, and agency partners to easily link all the data for police’s benefit.

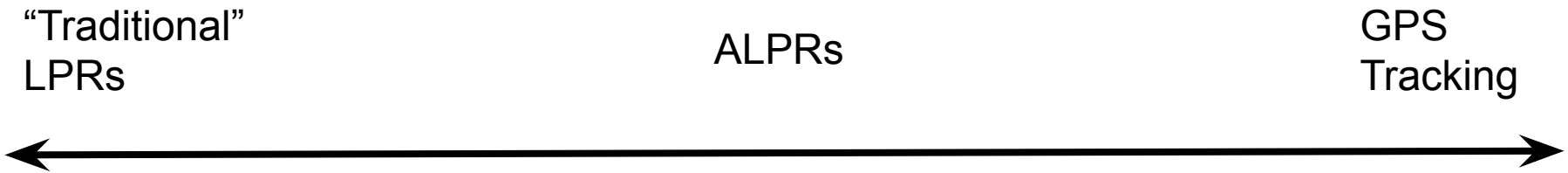
Not Just Your Car: The Vehicle-to-Person Pipeline



Not Just Your Car: The Vehicle-to-Person Pipeline



Where Flock Falls within the 4th Amendment Question



- Doesn’t track you
- Not considered a search
- No warrant needed

- Tracks you
- Not currently considered a search
- No warrant currently needed

Progressing through courts (Schmidt, et. al. v. City of Norfolk, et. al.)

- Tracks you
- Considered a search
- Warrant needed

What Circuit Courts are Saying

- Not really any 9th Circuit decisions around this issue recently
- 6th Circuit: *Taylor v. City of Saginaw* (April 22, 2019) No. 17-2126 (Link)
  - Tire chalking is a search and requires a warrant
- 4th Circuit: *Leaders of a Beautiful Struggle v. Baltimore Police Department.* 2 F.4th 330 (4th Cir. 2021) (Link)
  - “the access of data that in the aggregate allowed police to deduce an individual’s identity from the whole of their movements to be a search — as such, the warrantless use of such data violated the Fourth Amendment.”
- Virginia State Court of Appeals: *Schmidt, et. al. v. City of Norfolk, et. al.* (Link)
  - Recently ruled that Flock data does not require a warrant to access

This is part of a greater shift in how the government collects our data.

There was a time where government surveillance was conducted on an “as needed” basis. The information was collected only if they could prove they had reason to have it.

We are in, and still transitioning to, a time where information is collected without question and used for whatever purpose the government desires later.

What happens to your data once it’s entered into Flock’s Database

Flock’s Patented AI System: No. 11,416,545

Truly the core of it all - without this, all the cameras and gunshot detectors would be nothing more than simple cameras and microphones.

- Images & videos from cameras go into Flock’s AI systems
- The AI categorizes the information to fit into a “Vehicle Fingerprint”
  - This consists of vehicle plate #, make, model, year, color, accessories, damage, etc.
  - For their person-based technology: gender, race, height, weight, clothing, etc.
  - For shotspotter technology: gunshots, “human distress” (known to be terribly ineffective)
- Flock’s patent openly acknowledges that it can be trained to look for other criteria as well.
  - This is, after all, a fundamental aspect of artificial intelligence

Flock's Patented AI System cont.

- After information is categorized by the AI system, hotlist alerts are given for wanted & suspected vehicles
  - If your movement is deemed "suspicious", it will alert police (Link)
- Your "vehicle fingerprint" and all its characteristics are tagged and logged
- It is entered into the database, where it becomes searchable by Flagstaff PD and any other agency with data sharing access
  - Searching will be covered next, and data sharing is covered in the next section

Who Owns the Data?

The data is owned by the department that is leasing the camera that it was taken with. However, that data is just about useless without Flock Safety acting as the middle man. Flock also uses it to train their AI models.

As of October 19th, 2025, in the last 30 days:

- 415,434 unique cars were scanned & tracked by Flagstaff Flock cameras
- 1,811 scans resulted in a hotlist hit (~0.4%, which is higher than normal)
- 475 database searches were conducted by Flagstaff PD (~0.1%)

Conservatively assuming all database searches were separate from hotlist hits, ~99.5% of stored flock data is without cause after 30 days.

Causeless Mass/Dragnet Surveillance Breeds Abuse

When the government (or corporations) collect our data en masse for no reason, it is ripe for abuse, misuse, and even cybersecurity threats.

- In 2025, Flock and Motorola ALPR systems had cybersecurity breaches
  - Motorola exposed live data access to all their cameras to everyone
  - Flock exposed a misconfigured demo site that revealed source code and internal portals
- Texas police used Flock ALPRs to track a woman who had an abortion across state lines
- A police officer used Flock Safety ALPRs to stalk his estranged wife in Kechi, KS
- A police officer accepted a bribe to run a woman's license plate in Georgia
- A police officer used ALPRs to stalk his ex-girlfriend in Ohio
- California agencies keeping data longer than necessary and sharing it with unauthorized agencies

Who Pays When Flock Fails?

We do.

When Flock messes up, it often leads to guns-out altercations terrorizing families.

- San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error
- Cops Terrorize Black Family but Blame License Plate Reader for Misidentifying 'Stolen' Vehicle
- Deputies Sued After False ALPR Hit Leads To Guns-Out Traffic Stop Of California Privacy Activist
- Privacy advocate sues Contra Costa sheriff's deputies after license plate readers target his car stolen

In the end, taxpayers pick up the bill for Flock and PD’s mistakes. Flock has almost zero liability.

Additionally, Flock locks the city into its ecosystem, raising rates and essentially forcing us to go along.

Isn’t This for our Own Safety?

There is no independent research that ALPRs reduce crime.

- Flock Safety claims that 10% of reported crime in the US is solved by Flock technology
    - This study was conducted by two Flock employees “given legitimacy with the 'oversight' of two academic researchers whose names are also on the paper” - 404 Media Report

What research does exist regarding the ability of ALPRs to reduce crime is inconclusive at best:

- “Our findings indicate that, when small numbers of LPR patrols are used in crime hot spots in the way we have tested them here, they do not seem to generate either a general or offense-specific deterrent effect.”
    - - Journal of Experimental Criminology
- “There is not even a moderate degree of correlation between ALPRs and stolen vehicle recoveries, let alone any apparent causality”
    - - Automated License Plate Readers: A Study in Failure

How your data is shared with outside agencies

Two Forms of Sharing: 1:1 and the National Network

1:1 Sharing Agreements

Agencies can search by individual characteristics (make, model, color, accessories, etc).

Flagstaff PD has 1:1 agreements with 50/~65 agencies in Arizona.

Agencies with this access are listed on the transparency portal.

National LPR Network

Requires full license plate number.

Individual's most recent location automatically shared.

There are now an estimated 6,000 agencies that are a part of the National LPR Network.

Only 16 states have any laws regulating ALPR use - no, we're not one of them.

CA, IL, and VA do not allow out-of-state sharing.

Are not listed in transparency portal.

Immigration Policies Differ

- Flagstaff PD’s ALPR use policy outright denies use for immigration.
- They fully share their ALPR data with Coconino County Sheriff, who only denies to “solely” use a lookup for immigration purposes.
    - How much weaker are the policies of the 49 other agencies?
- National LPR Database lookups from others do not need to abide by these imposed immigration use restrictions.

What's the Risk of Federal Government Access?

They've already accessed it.

We know via Open Access Records and US Senator Ron Wyden that Border Patrol, ICE, Secret Service, and the Navy had direct access to the National LPR Network in 2025.

- This was denied for months by Flock, until in August they eventually backtracked, announced it was just a pilot program, and ended the program.
- Flock only admitted to Border Patrol, reporting on the rest came out last Thursday.
    - How much more do we not know?

ICE, ATF, DEA, and others have also obtained access via informal agreements with police agencies. This includes password sharing and lookup requests.

Going forward, Congress can pass a law mandating sharing. It could take as little as an executive order or simple pressure.

The National LPR Database is the most dangerous vector in the meantime.

Are there threats you see that I’m missing?

What can you do now?

Get Flock out of Flag!

Just by attending today you know more than 99%+ of people!

City Council Meeting: Oct. 28th, starts at 3pm

- Attend to show this is an important community issue
- SPEAK if you can!
  - In-person (preferred) or online
- If you cannot do the above, please write the council
  - Write to them anyways!

Flagstaff City Council Contact Information

Mayor Becky Daggett: becky.daggett@flagstaffaz.gov

Vice Mayor Miranda Sweet: miranda.sweet@flagstaffaz.gov

Councilmember Austin Aslan: austin.aslan@flagstaffaz.gov

Councilmember Lori Matthews: lori.matthews@flagstaffaz.gov

Councilmember Khara House: khara.house@flagstaffaz.gov

Councilmember Anthony Garcia: anthony.garcia@flagstaffaz.gov

Councilmember David Spence: david.spence@flagstaffaz.gov

Thank you!

Stay Connected on Instagram or TikTok: @flockoutofflag

Recommended resources:

deflock.me
eyesonflock.com
atlasofsurveillance.org
plateprivacy.com
haveibeenflocked.com